ABSTRACT OF THE DISCLOSURE

A method, apparatus and system for electronically verifying that a person using an electronic apparatus is who the person claims to be. It may be used for computers, e-commerce, financial transaction cards, automotive access and ignition, security badges, building access, cell phones and any other application in which electronic identification of a person is required. The security device in initiating a contact or in response to an inquiry as to identification transmits its public key identification number. The host encrypts a random message utilizing the user's public key identification number. Assuming the user is who the user claims to be, the user is able to decrypt the random message utilizing the user's corresponding private key. The private key never needs to be disclosed to anyone. The random message is changed with each use. The decrypted random message, which may preferably be a random number, is sent to the host, which upon favorable comparison with the random message sent to the user is able to verify that the user is the person he or she claims to be. All of this may be accomplished over unsecure lines without any requirement for a central controlling authority. The system may preferably be embodied in hardware which is detachable from any computer and transportable. However, it may be incorporated into software in a computer or the like.